Electronic Information & Communication Systems Policy

DOCUMENT CONTROL			POLICY LEVEL	Trust / **School** Statutory / **Non-statutory**
Approved by	Local Governing Body		Approved date	Autumn 2025
			Next review date	Autumn 2026
Published location	Sharepoint			
Version	Date issued	Author	Update information	
V1.0	01/09/2024	Alison Deadman		
V2.0	20/01/2026	Alison Deadman	Added in sections on monitoring email and monitoring use of internet	

Related policies:

- Bullet point related policies as a list

Contents

1. Introduction 2
2. Scope of the Policy 3
3. Prohibited use and breach of this policy 3
4. Equipment Security & Passwords 3
5. Systems Use & Data Security 4
6. Email Etiquette & Content 5
7. General Guidance 7
8. Emails- monitoring 8
9. Use of the Internet 10
10. Internet - monitoring 10
11. Personal Use of the School's System 11
12. Inappropriate Use of Equipment & Systems 11

1. Introduction

The school's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service. However, it also brings with it certain risks, some of which may involve potential legal and financial liabilities for both us and you, e.g:

- inadvertently entering into contracts or commitments on behalf of us;
- introducing viruses into our systems;
- breaching copyright or licensing rights;
- breaching data protection rights;
- breaching confidentiality and security;
- defamation; and/or
- bullying, harassment and discriminatory conduct.

This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the school who are required to familiarise themselves and comply with its contents. The school reserves the right to amend its content at any time.

This policy outlines the standards that the school requires all users of these systems to observe, the circumstances in which the school will monitor use of these systems and the action the school will take in respect of any breaches of these standards. We expect our computer and communications systems and equipment to be used in an effective and professional manner and encourage all staff to develop the necessary skills to achieve this. These systems and equipment are provided by us for the purpose of our business, and to assist staff in carrying out their duties effectively. It is the responsibility of all staff to ensure that these systems and equipment are used for proper business purposes and in a manner that does not compromise us or our staff in any way.

All staff should consider how their reputation and that of the School might be affected by how they communicate and conduct themselves online.

The use by staff and monitoring by the school of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The school is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect

the school's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the school's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The school has the right to monitor all aspects of its systems, including data which is stored under the school's computer systems in compliance with the GDPR.

2. Scope of the Policy

This policy applies to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, governors, trustees, consultants and other contractors who have access to our computer and other communications systems. It also applies to personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated us.

This policy applies to the use (or misuse) of computer equipment, e-mail, internet systems, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail but it applies equally to the use of fax machines, copiers, scanners, and the like, both in the workplace and from outside (e.g. via remote access).

3. Prohibited use and breach of this policy

We consider this policy to be extremely important. Any breach of the policy will be dealt with under our disciplinary policy. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw an individual's internet and/or email access.

Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

- unauthorised use of the internet;
- creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;
- creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our equality, diversity and inclusion policies;
- accessing, transmitting or downloading any confidential information about the School and/or any of our staff and/or current, former or prospective pupils or parents, suppliers, contractors or other such third parties, except where authorised in the proper performance of your duties;
- accessing, transmitting or downloading unauthorised software; and
- viewing, accessing, transmitting or downloading any material in breach of copyright.

4. Equipment Security & Passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken

and which contains at least 6 characters including both numbers and letters. Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the IT managed service provider as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the school e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the MSP Sweethaven

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The school reserves the right to require employees to hand over all school data held in computer useable format.

Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), PDA or smart phone must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers. If staff take devices off-site they should follow the Home Working Policy.

5. Systems Use & Data Security

Members of staff should not delete, destroy or modify any of the school's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the school's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the MSP Sweethaven who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other

device to our systems or network without express prior permission from the Headteacher. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this
All members of staff need to inform the Headteacher before sharing any data with any third parties so the School can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given all files and data should always be virus checked before they are downloaded onto the school's systems. If in doubt, the employee should seek advice from the MSP Sweethaven or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;
- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of the MSP Sweethaven or Senior Leadership Team. This includes, but is not limited to, any smart phone or telephone, iPad, laptop (or other mobile device tablet), USB device, i-pod, digital camera, infra red connection device or any other device.

The school monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The MSP Sweethaven should be informed immediately if a suspected virus is received. The school reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The school also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "E-mail etiquette and content" below.

6. Email Etiquette & Content

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The school's e-mail facility is intended to promote effective communication within the business on matters relating to the school's business activities and access to the school's e-mail facility is provided for work purposes only.

Staff are permitted to make occasional and reasonable personal use of the school's e-mail facility provided

such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the school's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The school encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the school's best practice.

Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the school. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the school in the same way as the contents of letters or faxes.

Staff should check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information and amount to a breach of data protection.

All members of staff should remember that e-mails can be the subject of legal action for example, in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The school standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote

access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages or which otherwise:-

- May be inconsistent with our equality, diversity inclusion and anti harassment and bullying policies;
- criticise other schools or their staff; or
- state that anyone is incompetent.

This list is not exhaustive.

If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied or are offended by material sent to you by a colleague via e-mail, you should inform the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the school's formal grievance procedure. (Further information is contained in the School's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

7. General Guidance

As general guidance, staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the school;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection,

unless it is clear that the owner of such works allows this;

- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature;

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once and not forward it to any internal or external recipient, other than internally to the data protection officer in order to report a breach of this or another policy. If you believe you may have been bullied, harassed, sexually harassed or victimised, we encourage you to report this. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The headteacher should be informed as soon as reasonably practicable.

8. Emails- monitoring

We may monitor the email and instant messaging systems or network in the workplace for the following reasons:to determine whether they are communications relevant to the carrying on of our relevant activities;

- if the individual is absent from work, to check communications for business calls to ensure the smooth running of the School;
- to record transactions;
- where we suspect that the individual is sending or receiving messages that are:
    - detrimental to us;
    - in breach of the individual's contract, or this policy;
    - in breach of data protection rights;
    - to monitor staff conduct;
    - to investigate complaints, grievances or criminal offences.

When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

- look at the sender or recipient of the email and the subject heading only; and
- avoid opening emails marked 'Private' or 'Personal'.

We do not, as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of its systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, we carry out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

We will only intercept (i.e. open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

- to determine whether the message is relevant to the carrying on of our business;
- to establish the existence of facts;
- to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system;
- to check whether staff using the system in the course of their duties are achieving the standards required of them;
- for the purpose of investigating or detecting the unauthorised use of the system;
- for the purpose of preventing or detecting crime; or
- for the effective operation of the telecommunication system.

The content of emails will be examined only in exceptional circumstances, initially by the Headteacher The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the School believes there may have been a breach of the individual's contract or this Policy.

9. Use of the Internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the school, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the school's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the school's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use school systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The school's website may be found at www.WindrushCharltonprimary.org. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The school should refrain from texting and using systems such as WhatsApp for school related matters using personal phones. The school require staff to use alternative systems to make contact with staff (such as emails).

The school has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the school and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the school. Any exceptions to this must be authorised by Jo Marchant-Trust Lead-who will liaise with the Senior Leadership Team as appropriate and necessary.

10. Internet - monitoring

We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that the individual has been using the internet in breach of the individual's contract or this policy, e.g.:

- by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us;
- by spending an excessive amount of time viewing websites that are not work-related.

Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using our systems or network and internet usage using hand-held or portable electronic

devices.

Monitoring will normally be conducted by our MSP Sweethaven. The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the MSP Sweethaven believes there may have been a breach of the individual's contract or this Policy.

11. Personal Use of the School's System

The school permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

- Use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);
- Personal e-mails must be labelled "personal" in the subject header;
- Use must not interfere with business or office commitments;
- Use must not commit the school to any marginal costs;
- Use must comply at all times with the rules and guidelines set out in this policy;
- Use must also comply with the school's compliment of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Excessive or inappropriate personal use of the school's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The school reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

12. Inappropriate Use of Equipment & Systems

Incidental/occasional and reasonable personal use is permissible provided it is in full compliance with the school's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure)

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this

list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- Transmitting a false and/or defamatory statement about any person or organisation;
- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
- Transmitting confidential information about the school and any of its staff, students or associated third parties;
- Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the school);
- Downloading or disseminating material in breach of copyright;
- Copying, downloading, storing or running any software without the express prior authorisation of the Headteacher and MSP Sweethaven
- Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- Forwarding electronic chain letters and other materials;
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the school may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.